UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

52197 7590 12/09/2010

Wall & Tong, LLP
SRI INTERNATIONAL
25 James Way
Eatontown, NJ 07724

EXAMINER	
SHERR, CRISTINA O	
ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 12/09/2010

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,788	08/31/2001	Alfonso De Jesus Valdes	SRI/4190-4	1821

TITLE OF INVENTION: PROBABILISTIC ALERT CORRELATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$300	$0	$1810	03/09/2011

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

52197 7590 12/09/2010

Wall & Tong, LLP
SRI INTERNATIONAL
25 James Way
Eatontown, NJ 07724

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,788	08/31/2001	Alfonso De Jesus Valdes	SRI/4190-4	1821

TITLE OF INVENTION: PROBABILISTIC ALERT CORRELATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$300	$0	$1810	03/09/2011

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHERR, CRISTINA O	3685	705-026000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,788	08/31/2001	Alfonso De Jesus Valdes	SRI/4190-4	1821

52197 7590 12/09/2010

Wall & Tong, LLP
SRI INTERNATIONAL
25 James Way
Eatontown, NJ 07724

EXAMINER	
SHERR, CRISTINA O	
ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 12/09/2010

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 133 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 133 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	Application No.	Applicant(s)	
	09/944,788	VALDES ET AL.	
	Examiner	Art Unit	
	CRISTINA SHERR	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Appeal Brief filed 8/18/2010*.

2. ☒ The allowed claim(s) is/are *1,2,7,8,13 and 14*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____.
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. This Office Action is in response to the Appeal Brief filed August 18, 2010.

Claims 1-30 are currently pending in this case.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

3. Authorization for this examiner's amendment was given in a telephone interview with Diana Rea, reg.no. 54,938, on November 12, 2010.

4. The claims are hereby amended as follows:

1. (Currently Amended) In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing the alerts into alert classes, both the alerts and the alert classes having a plurality of features, the method comprising:

(a) receiving a new alert;

(b) identifying a set of similar features shared by the new alert and one or more existing alert classes;

(c) updating, using a processor, a threshold similarity requirement for one or more of the similar features;

(d) updating, using a processor, a similarity expectation for one or more of the similar features;

(e) comparing, using a processor, the new alert with the one or more existing alert classes, using a similarity measure Sim(X,Y) that expresses a similarity between the new alert and a given one of the one or more existing alert classes, where SIM(X,Y) is defined as:

$$Sim(X,Y) = \frac{\left[\sum_{C \in X \text{ and } C \in Y} P_X(C) \times P_Y(C)\right]^2}{(P_X \cdot P_X)(P_Y \cdot P_Y)}$$

where X is a set of features and probability values for the new alert, Y is a set of features and probability values for the given one of the one or more existing alert classes, $P_X(C)$ is a probability of a category C in X, $P_Y(C)$ is a probability of the category C in Y, P_X is a probability vector over one or more categories observed for X, and P_Y is a probability vector over one or more categories observed for Y; and either:

(f1) associating, using a processor, the new alert with a one of the one or more existing alert classes that the new alert most closely matches according to the similarity measure; or

(f2) defining, using a processor, a new alert class that is associated with the new alert[[,]]

~~wherein at least one of: the receiving, the identifying, the updating a threshold similarity, the updating a similarity expectation, the comparing, the associating, or the defining is performed by a processor~~.

2. (Previously Presented) The method of claim 1 further comprising a step (a1) of passing each of the one or more existing alert classes through a transition model to generate a new prior belief state for each of the one or more existing alert classes.

3. – 6. (Cancelled)

7. (Currently Amended) A computer readable storage medium containing an executable program for organizing alerts that are generated by a plurality of sensors into alert classes, both the alerts and the alert classes having a plurality of features, where the program, when executed by a processor, causes the [a] processor to perform steps of:

(a) receiving a new alert;

(b) identifying a set of similar features shared by the new alert and one or more existing alert classes;

(c) updating a threshold similarity requirement for one or more of the similar features;

(d) updating a similarity expectation for one or more of the similar features;

(e) comparing the new alert with the one or more existing alert classes, using a similarity measure Sim(X,Y) that expresses a similarity between the new alert and a given one of the one or more existing alert classes, where SIM(X,Y) is defined as:

$$Sim(X,Y) = \frac{\left[\sum_{C \in X \text{ and } C \in Y} P_X(C) \times P_Y(C)\right]^2}{(P_X \cdot P_X)(P_Y \cdot P_Y)}$$

where X is a set of features and probability values for the new alert, Y is a set of features and probability values for the given one of the one or more existing alert classes, $P_X(C)$ is a probability of a category C in X, $P_Y(C)$ is a probability of the category C in Y, P_X is a probability vector over one or more categories observed for X, and P_Y is a probability vector over one or more categories observed for Y; and either:

(f1) associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches according to the similarity measure; or

(f2) defining a new alert class that is associated with the new alert.

8. (Previously Presented) The computer readable storage medium of claim 7 further comprising a step (a1) of passing each of the one or more existing alert classes through

a transition model to generate a new prior belief state for each of the one or more existing alert classes.

9. – 12. (Cancelled)

13. (Currently Amended) In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a system for organizing the alerts into alert classes, both the alerts and the alert classes having a plurality of features, where the system comprises:

(a) means for receiving a new alert;

(b) means for identifying a set of similar features shared by the new alert and one or more existing alert classes;

(c) means for updating a threshold similarity requirement for one or more of the similar features;

(d) means for updating a similarity expectation for one or more of the similar features;

(e) means for comparing the new alert with the one or more existing alert classes, using a similarity measure Sim(X,Y) that expresses a similarity between the new alert and a given one of the one or more existing alert classes, where SIM(X,Y) is defined as:

$$Sim(X,Y) = \frac{\left[\sum_{C \in X \text{ and } C \in Y} P_X(C) \times P_Y(C)\right]^2}{(P_X \cdot P_X)(P_Y \cdot P_Y)}$$

where X is a set of features and probability values for the new alert, Y is a set of features and probability values for the given one of the one or more existing alert classes, $P_X(C)$ is a probability of a category C in X, $P_Y(C)$ is a probability of the category C in Y, P_X is a probability vector over one or more categories observed for X, and P_Y is a probability vector over one or more categories observed for Y; and

(f1) means for associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches according to the similarity measure, or defining a new alert class that is associated with the new alert.

14. (Previously Presented) The system of claim 13 further comprising (a1) means for passing each of the one or more existing alert classes through a transition model to generate a new prior belief state for each of the one or more existing alert classes.

15. – 30. (Cancelled)

Reasons for Allowance

5. Claims 1-2, 7-8, and 13-14 are allowed.

6. The following is the Examiner's statement of reasons for allowance:

7. Regarding the claimed terms, Applicant is reminded that a "general term must be understood in the context in which the inventor presents it." *In re Glaug* 283 F.3d 1335, 1340, 62 USPQ2d 1151, 1154 (Fed. Cir. 2002). Therefore the Examiner must interpret the claimed terms as found on pages 1-59 of the specification. Clearly almost all the general terms in the claims may have multiple meanings. So where a claim term "is susceptible to various meanings . . . the inventor's lexicography must prevail . . . ." *Id*. Using these definitions for the claims, the claimed invention was not reasonably found in the prior art.

8. The primary reference Nine et al (US 6,560,611) discloses as previously discussed. Nine, however, does not disclose at least comparing, using a processor, the new alert with the one or more existing alert classes, using a similarity measure

Sim(X,Y) that expresses a similarity between the new alert and a given one of the one or more existing alert classes, where SIM(X,Y) is defined as:

$$Sim(X,Y) = \frac{\left[\sum_{C \in X \text{ and } C \in Y} P_X(C) \times P_Y(C)\right]^2}{(P_X \cdot P_X)(P_Y \cdot P_Y)}$$

where X is a set of features and probability values for the new alert, Y is a set of features and probability values for the given one of the one or more existing alert classes, $P_X(C)$ is a probability of a category C in X, $P_Y(C)$ is a probability of the category C in Y, P_X is a probability vector over one or more categories observed for X, and P_Y is a probability vector over one or more categories observed for Y. Moreover, the missing claimed feature is not likely to be found in a reasonable number of references.

9. For these reasons, independent claims 1, 7, and 13 and their dependent claims 2, 8, and 14 are deemed allowable.

10. Any comments considered necessary by Applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CRISTINA SHERR whose telephone number is (571)272-6711. The examiner can normally be reached on 8:30-5:00 Monday through Friday.

12. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin L. Hewitt, II can be reached on (571)272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

13. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CRISTINA OWEN SHERR
Examiner
Art Unit 3685

/Calvin L Hewitt II/

Supervisory Patent Examiner, Art Unit 3685